IEEE EuroS&P: The Younger Sibling Across the Pond Following in Oakland's Footsteps

Terry Benzel | University of Southern California Information Sciences Institute
Frank Stajano | University of Cambridge

In a continued effort to bring some of the symposium to a wider audience, *IEEE Security & Privacy*'s Editorial Board devotes one special issue each year to highlight selected papers. Those in this issue are from the European conference held in Stockholm in 2019. Our first article develops a black-box penetration testing tool, based on machine learning, that was able to detect 35 new Cross-Site Request Forgery vulnerabilities on 20 major websites. The next article develops a smart contract platform with much better performance and confidentiality guarantees than the state of the art. A third article details how Spectre-like attacks could extract secrets from Intel's Software Guard Extensions secure enclaves. A fourth article develops an elaborate server-side countermeasure against online password guessing. Our final article, originally from the "Systematization of Knowledge" track, discusses the issue of inappropriate use of performance benchmarks in security papers, drawing examples from 50 papers published in the four top-tier security conferences, and suggests possible ways forward.

The IEEE European Symposium on Security and Privacy (EuroS&P) series was established in 2016 as the European counterpart of the prestigious and long-standing IEEE Symposium on Security and Privacy. In recent years it has become one of the top venues for security research in Europe and worldwide. The fourth edition of the conference was held at the KTH campus in Stockholm, Sweden, from 17 to 19 June 2019. It attracted 210 submissions, more than in any previous year. Based on the results of a rigorous double-blind, peer-review process from a program committee of more than 50 members, 42 of the 210 submissions were eventually selected, for an acceptance rate of 20%. The accepted papers covered many different areas in the broad field of security, and we have picked five of them for this special issue as representative samples, spanning from machine learning-assisted discovery of web vulnerabilities through high-performance and high-security smart contracts on blockchain, secure enclaves, and password-guessing countermeasures, all the way to the improper use of benchmarks in security papers.

A Fertile Field

We invited the authors of selected papers to submit a revision targeted to the broader magazine audience and enhanced with new results since the original paper's publication. We chose papers based on general interest and accessibility.

One of the papers in our selection is from the symposium's Systemization of Knowledge (SoK) track, which encourages work that evaluates, systematizes, and contextualizes existing knowledge. SoK papers provide a high value to the community but might not be accepted for publication in the symposium proceedings because of a potential lack of novel research contributions. Nonetheless, SoK papers analyze the current research landscape—identifying areas that have enjoyed much research attention, pointing out areas with unsolved challenges, and presenting a prioritization that can guide researchers solving important challenges. This sort of contribution is particularly valuable for *IEEE Security & Privacy*'s broad readership.

Digital Object Identifier 10.1109/MSEC.2020.2980180
Date of current version: 14 May 2020

In This Issue

Stefano Calzavara, Mauro Conti, Riccardo Focardi, Alvise Rabitti, and Gabriele Tolomei develop a browser plug-in for semiautomatic penetration testing of web sites in "Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery." Their plug-in, intended to be used by a security analyst, is powered by a machine learning classifier that identifies security-sensitive HTTP requests and feeds them to appropriate per-class vulnerability-detection heuristics.

Fan Zhang, Warren He, Raymond Cheng, Jernej Kos, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song bring high performance to smart contracts by combining the complementary properties of blockchain and hardware-based trusted execution environments in "The Ekiden Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts."

Guoxing Chen, Sanchuan Chen, Yuan Xiao, Yinqian Zhang, Zhiqiang Lin, and Ten-Hwang Lai give a detailed account of their application of Spectre techniques to the extraction of secret keys from Intel's Software Guard Extensions (SGX) enclaves in "SgxPectre: Stealing Intel Secrets From SGX Enclaves via Speculative Execution." They develop a program analysis tool through which they detect exploitable code patterns in several popular SGX runtime libraries. They then reevaluate whether the attacks still work after patching the CPU with Intel's latest microcode updates.

Yuan Tian, Cormac Herley, and Stuart Schechter develop a server-side account protection in "StopGuessing: Using Guessed Passwords to Thwart Online Password Guessing." In their technique, IP addresses that repeatedly guess the incorrect password for an account are blocked from logging in, but the number of failed attempts that triggers the block is modulated by the incorrect passwords previously submitted, penalizing those that look like password guesses but not those that look like typos of the actual password. They invest extra care to ensure that a compromise of the database of encrypted login credentials, now containing information about possible typos, won't make the offline cracking of the actual passwords any easier than before.

Erik van der Kouwe, Gernot Heiser, Dennis Andriesse, Herbert Bos, and Cristiano Giuffrida argue in their SoK paper that "Benchmarking Flaws Undermine Security Research." They introduce a taxonomy of 22 specific flaws, arranged in six groups, and apply it to 50 papers that had been accepted at four top-tier security conferences in 2010 and 2015. They report on the frequency of occurrence of each flaw and on the impact of the most frequently occurring flaws. They then offer suggestions on how to improve the situation, aimed at authors, program committees, and the community in general. The witty Sweden-themed slides that accompanied the presentation of the original article in Stockholm are also worthy of mention as among the most entertaining of the conference.

We hope that by bringing a piece of the European symposium to you, *IEEE Security & Privacy* will enhance the value of both the symposium (in its two geographical manifestations) and the magazine to the community. If you're able to attend, we look forward to seeing you at the 2020 symposium in Genova, Italy, and connecting with you through the pages of the magazine throughout the year. ■

Terry Benzel is the director of the Networking and Cybersecurity Research Division at the University of Southern California Information Sciences Institute. Contact her at tbenzel@isi.edu.

Frank Stajano is a professor of security and privacy and the head of the Academic Center of Excellence in Cyber Security Research at the University of Cambridge. He served as program cochair of IEEE EuroS&P with Frank Piessens of KU Leuven in 2019 and with Lujo Bauer of Carnegie Mellon University in 2020. Contact him at frank.stajano@cst.cam.ac.uk.

Editors' Note

In March 2020, the IEEE postponed the IEEE European Symposium on Security and Privacy 2020 as a precautionary measure against COVID-19 with the statement reproduced below. However, the situation is still in flux at the time this issue is going to press and plans might have changed again by the time you read this. Please consult the website https://www.ieee-security.org/TC/EuroSP2020/ for up-to-date information. We look forward to meeting you there once international travel is no longer risky.

> *The IEEE European Symposium on Security and Privacy 2020 conference is being rescheduled to September 7–11, 2020, in Genova, Italy. The IEEE has been monitoring the developing COVID-19. The safety and well-being of the IEEE European Symposium on Security and Privacy 2020 conference participants is our priority. After studying and evaluating the announcements, guidance, and news released by relevant national departments, the conference is tentatively rescheduled for September 7–11, 2020, in Genova, Italy. However, the situation may have changed by the time you read this. We are considering an online-only event, like S&P is doing in May. All options are open. We thank you for your understanding.*